ArcSight

Content Exchange in ESM

Gabriel Coelho-Kostolny
Software Development Manager
September 2008

Outline

- Resource Refresher
- Resource Archives
- Packages
- Import & Export Formats
- Exporting Data & Resources
- Importing Data & Resources
- Other Useful Tools & Options
- Be Aware (Gotchas)
- Q & A

Resource Refresher

What Are Resources?

- "Resources" are used for persistence & sharing of configuration details for some aspect of ESM
- Active Channels, Dashboards, Data Monitors, Rules, Reports, etc.
- ESM refers to these entities as "Resources"
  - All have common attributes
  - Each type has type-specific attributes as well
- Think of Resources as equivalent to file types
  - PowerPoint vs. Word vs. Excel

Universal Attributes

- Each Resource type will always have these attributes
  - ID – Unique (per manager) global ID
  - Name – Human-readable identifier for the resource
    - Names must be unique within a given group in ESM
  - Alias – An alternate name, also used for localization
    - Aliases must also be unique within a given group
  - Type – Internal, not used in the UI
- There are other universal attributes, but they aren't too interesting for the purposes of this talk

Where Do Resources Live in ESM?

- Each type has its own tree hierarchy in ESM
  - `/All Active Channels/`
  - `/All Zones/`
  - etc.
- Base resource attributes are stored in ARC_RESOURCE in the database
  - Resource-specific attributes are stored in separate tables
  - E.g. ARC_REPORT

Relationships

- Parent/Child
- Dependency
- Attachment

- Example: Report/Query/Filter/Template

- The ARC_RELATIONSHIP table is the repository for these relationships between resources

Resource Archives

A Word about Resources & Archives

- Archives, and Packages, are all about Resources and Resource relationships
- Resource relationships can save you work and pain
  - If you understand them
- Keys to the Archive/Package kingdom
  - Group parent/child relationships
  - Resource dependency relationships
- More on this later

What's a Content Archive?

- Original resource transportation mechanism for ESM
- Text-based XML format
- Composed of
  - Configuration Section (`ArchiveCreationParameters`)
  - Resource Serializations
- Advantages
  - Easy to move around
  - Text-based diffing
- Disadvantages
  - Sometimes challenging to configure/understand

Used with “Archive Tool”

- `$ARCSIGHT_HOME\bin\arcsight archive`
- Common actions
  - `import`
  - `export`
  - `list`
- Supports a semi-interactive mode
- Allows passing in a previous archive to provide export parameters

Export Parameters (Ain't They Gorgeous?)

```
<ArchiveCreationParameters>
  <exclude>
   <list>
    <ref type="Group" uri="/All Filters/ArcSight System/"
      id="0gRTVGAwBABCFEGvLDCwdyQ==/>
   </list>
  </exclude>
  <excludeChildren>
   <list>
    <ref type="Group" uri="/All Asset Categories/“
      id="0100010001000103l"/>
   </list>
  </excludeChildren>
  <excludeChildrenIfNotIncluded>
   <list>
    <ref type="Group" uri="/All Filters/ArcSight
      Foundation/Configuration Monitoring/"/>
   </list>
  </excludeChildrenIfNotIncluded>
```

Export Parameters - continued

```
  <excludeReferenceIDs/>
  <excludeTypes>
   <list>
    <string>Agent</string>
   </list>
  </excludeTypes>
  <format>export</format>
  <include>
   <list>
    <ref type="Group" uri="/All Filters/ArcSight
    Foundation/Common/Anti-Virus/"/>
   </list>
  </include>
</ArchiveCreationParameters>
```

ArcSight™

Packages

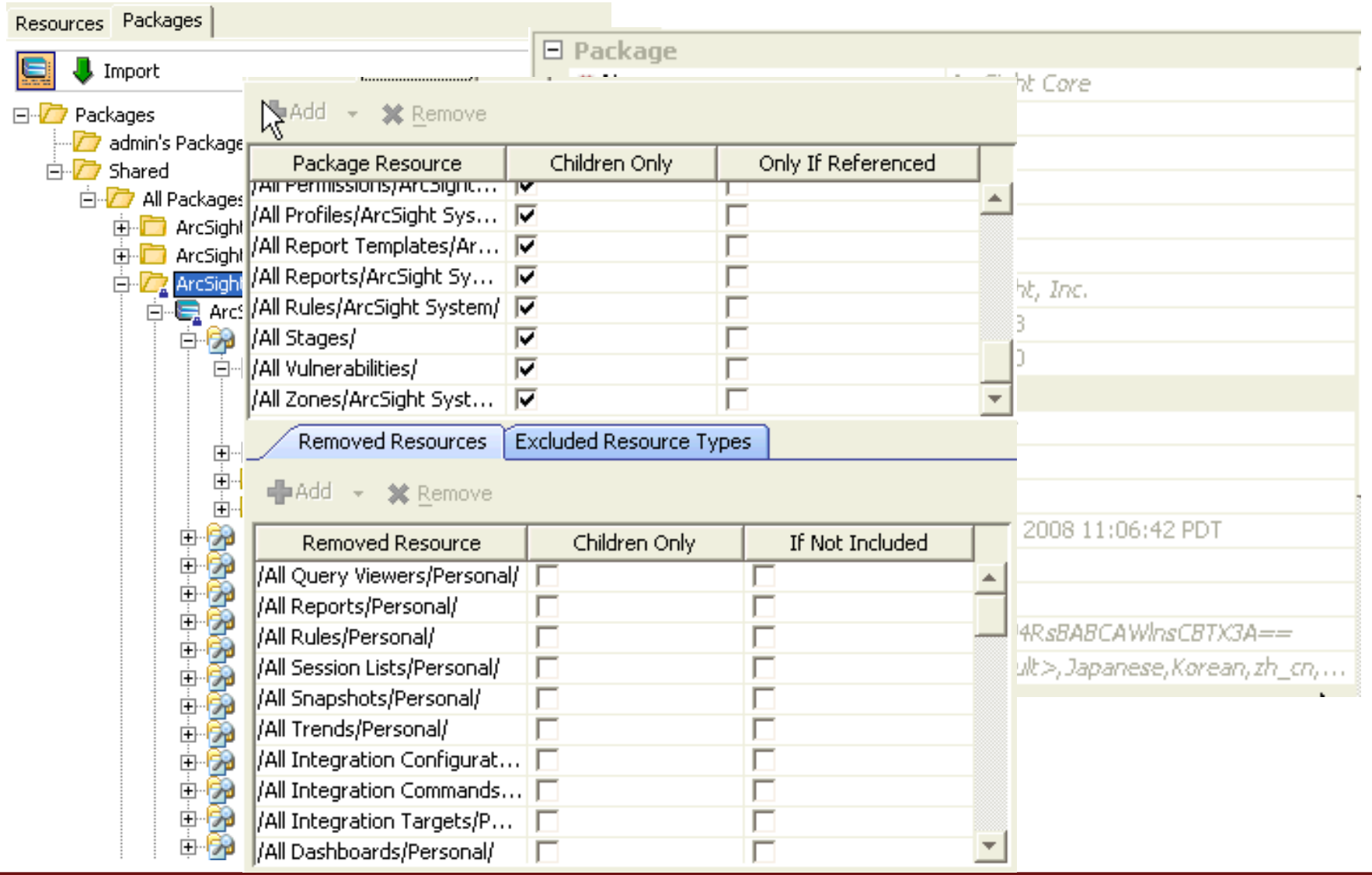
What's a Package?

- "Package" often refers to two different things
  - Package Resource
  - Package Bundle
- Resource is editable and viewable in ESM Console
  - Provides an interactive editing & exploration view
- Bundle is the physical manifestation of the Package
  - ZIP file – uses ".ARB" extension
  - Manifest
  - 1 or more XML archives (per-Package)

What's in a Package (Resource)?

- `ArchiveCreationParameters` in the form of a resource
- With a few added sweeteners:
  - Name
  - Description
  - GUI viewer/editor
  - Nicer physical bundling
  - Versioning
  - Inter-package dependencies

Packages View



ArcSight™

Import & Export Formats

Formats

- Formats tell the system how to export (serialize) resources into XML
  - What attributes to include
  - Whether to include data (e.g. Active Lists)
- Formats also instruct the system on import behavior, but this is primarily of use to ArcSight-internal folks
- Format definitions are located in:
  - `$ARCSIGHT_HOME\config\archive`
- Formats can be defined on a per-resource basis in:
  - `$ARCSIGHT_HOME\config\archive\handler`

Export Formats

- Choose based on:
  - What resources should be exported
  - What attributes should be included in the export
  - What relationships should be included in the export
  - Whether data should be included in the export
- Common formats:
  - `export` – excludes list entries, other data
  - `default` – brings along list entries
  - `xml.external.case` – designed for export to external systems, brings cases with associated events

Exporting Data & Resources

What Can You Export?

- Resource definitions
- Resource relationships
- Data associated with resources
  - Active Lists
  - Session Lists
  - Cases
- Some things you might not expect

Resource Definitions

- Standard behavior
  - This is the “classic” use case for export
- Select the appropriate format for the things you want
- Specify what groups or resources
- Export!
- You land yourself a nice XML file
  - Store it
  - Share it
  - Diff it

Resource Data

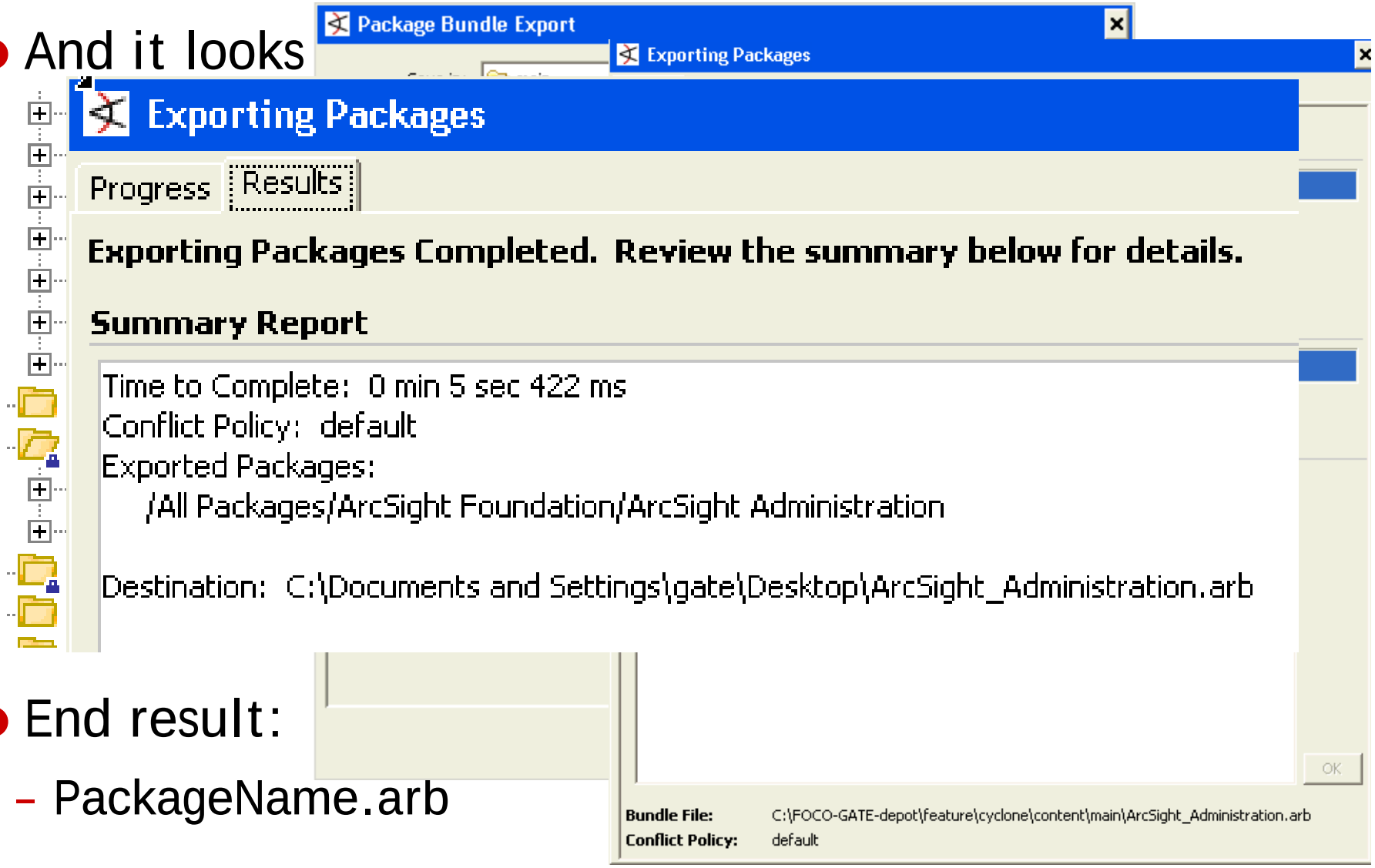
- Active List entries
  - Useful if you have a long-lasting list of things that you'd like to preserve or share
- Session List entries
  - Useful if you have a long-lasting list of things that you'd like to preserve or share
- Cases
  - Useful for export to other case management systems
  - This includes *full XML Event dumps*

Uses for Exports

- Back up your content
- Share content with others
- Diff changes to your ESM resources
- Review data in Lists
- Export Cases for use elsewhere, or for historical reasons
- Leverage Event data outside ESM
- … Profit!

Exporting with Packages

- And it looks



- End result:
  - PackageName.arb

Exporting with Archives

- **$ARCSIGHT_HOME\bin\arcsight archive**
  - **-action export -format (export|default)**
  - **[-param PrevExport.xml] -u <username>**
  - **-p <password> -f <archive>.xml –m <mgr>**
- End result:
  - <archivename>.xml
- Best way to learn how to create these is to export some and look at what you get
- Also look at the `<ArchiveCreationParameters/>` element created in packages you export to bundles

Case & Event Example

- Specify one particular case and pass file in as the
  - `–param` value for the export
- Also note the format is `xml.external.case`

```
<ArchiveCreationParameters>
  <format>xml.external.case</format>
  <include>
   <list>
   <ref type="Case“
        uri="/All Cases/Personal/admin's Cases/test case“
        id="7xzGx5xsBABCOEQ+GvuxBsQ==“/>
   </list>
```

Yields You…

- Case ID='7xzGx5xsBABCOEQ+GvuxBsQ==' URI='/All Cases/Personal/admin's Cases/test case‘
- SecurityEvent ID='190000009134‘
- SecurityEvent ID='190000009135'
- SecurityEvent ID='190000009136'
- SecurityEvent ID='190000009137'

- Entry counts by type:
- Case: 1
- SecurityEvent: 4
- Total entries in the archive: 5

ArcSight™

Importing Data & Resources

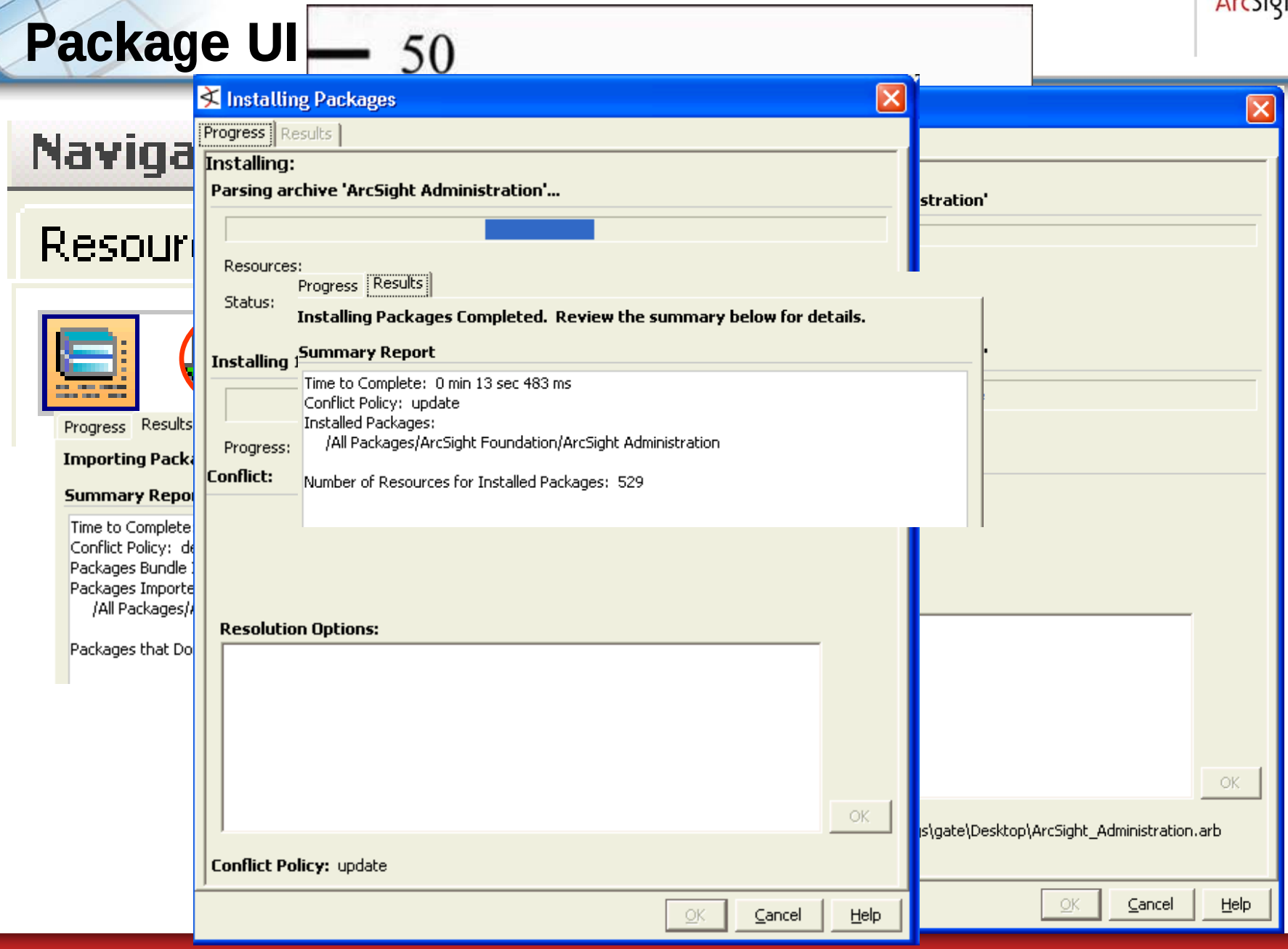
Uses for Resource Imports

- Load resources from elsewhere into your ESM
- Reconfigure resources
- Populate existing resources with data
- Create new resources based on outside data

Import Mechanisms

- Console UI
  - Active List Import
- Packages UI
  - Most useful for things directly exported from a Console
  - Easy to use
  - Good management capabilities
  - Versioning
  - Packages command-line tool also available
- Archive Tool
  - Command-line based
  - Useful for slightly less traditional tasks
  - Exposes more advanced capabilities

Package UI


Installing Packages
Progress
Results
Installing:
Parsing archive 'ArcSight Administration'...
Resources:
Progress
Results
Status:
Installing Packages Completed. Review the summary below for details.
Summary Report
Time to Complete: 0 min 13 sec 483 ms
Conflict Policy: update
Installed Packages:
/All Packages/ArcSight Foundation/ArcSight Administration
Number of Resources for Installed Packages: 529
Progress:
Conflict:
Resolution Options:
OK
Conflict Policy: update
OK
Cancel
Help
stration'
s\gate\Desktop\ArcSight_Administration.arb
OK
Cancel
Help

Command-line Package Import

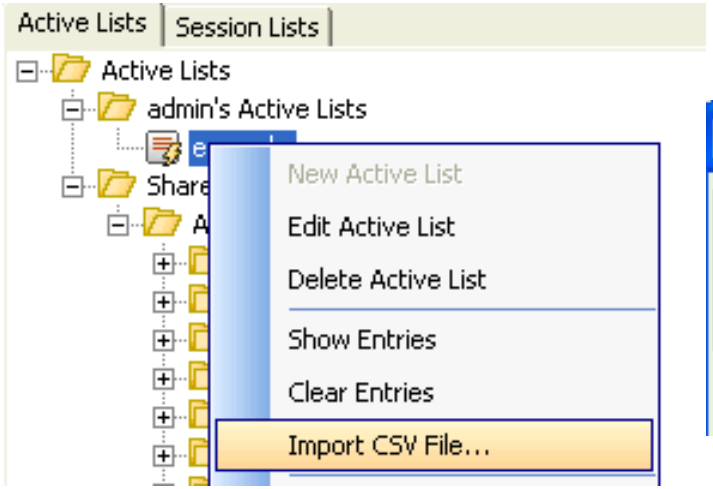
- $ARCSIGHT_HOME\bin\arcsight package
- -action install -f “<package>.arb“
- -m <manager> -u <user> -p <password>
- -package “/All Packages/<URI for package>”

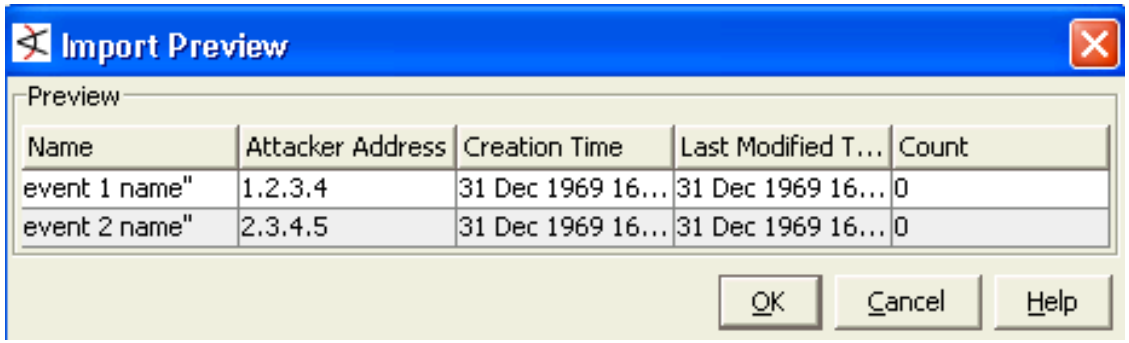
Command-line Archive Import

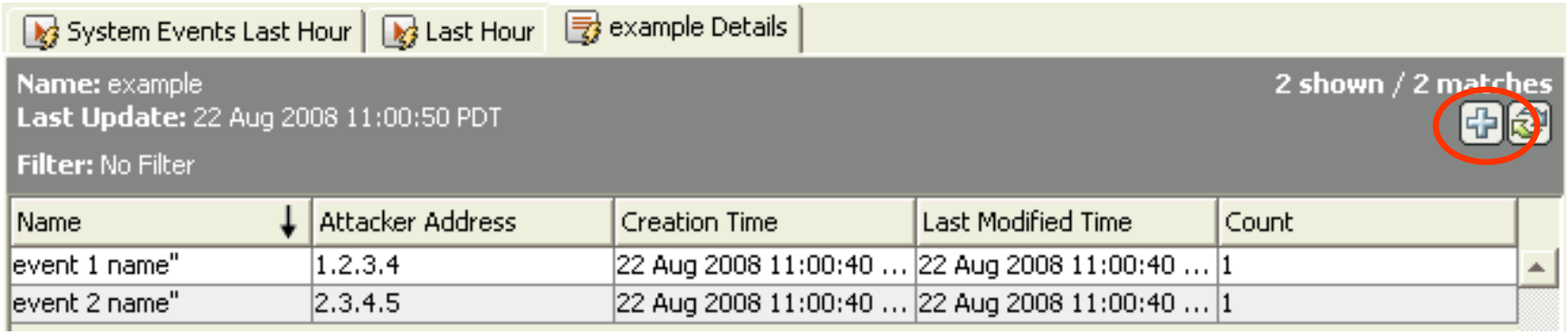
- `$ARCSIGHT_HOME\bin\arcsight archive`
- `-action import -format default`
- `-f <archive name> -m <manager>`
- `-u <username> -p <password>`

UI-Based Alternatives

- Active List import in Console UI







Including Data in Archives & Packages

- Use format “default”
- Include your list in the Package or archive parameters
- Et voila:

```
<ActiveList id="HF+CQ6xsBABCoLQ+GvuxBsQ==" name="example" action="insert" >
    <activeListEntries>
      <list>
       <map>
        <count>1</count>
        <creationTime>1219428040000</creationTime>
        <lastModifiedTime>
              1219428040000</lastModifiedTime>
        <values>
         <list>
```

ArcSight™

Other Useful Tools & Options

GUI Views

- Graph View
  - Configurable
  - Shows you resource relationships & dependencies
  - Print it out for reference
- Package View
  - Show full listing with dependencies
  - Show just directly linked resources
  - Diff with the previously exported Package

Archive List

- `$ARCSIGHT_HOME\bin\arcsight archive`
- `-action list -f <archive>.xml`
  - Provides a listing of the Name, URI, Type, ID of every resource in the XML archive
- Available in the Packages UI as well
  - Also allows you to diff between current and saved package contents

Packages

- Packages can contain any resource type
  - For instance, File resources
- You can use packages to bundle up Files that you'd like to make available to all Console users
- User simply goes to the File resource and saves it to their local system
  - Files should be relatively small
  - Default limit for total File resource space is 300MB

ArcSight™

Be Aware (Gotchas)

Testing & Caution

- Package and archive imports can make your system unusable unless you exercise due care
- Test things in a non-production environment before deployment
- Import and install packages & archives as the user with the least privileges necessary
- Ryan has a great talk on content development best practices
  - SN16: Content Development Best Practices

Hand-Created Archives Can Be Dangerous

- Caution is even more important
- Be very sure about what you're creating
- Test and test again
  - On more than one system!

Don’t Export Standard Content Resources

- When creating Packages or archives, exclude ArcSight-provided resources
  - You may overwrite things unintentionally
  - You may encounter permissions problems when importing
- Exclude by URI:
  - `/All <Resource>/ArcSight System`
  - `/All <Resource>/ArcSight Administration`
  - `/All <Resource>/ArcSight Foundation`
  - `/All <Resource>/ArcSight Solutions`

ArcSight™

Q & A

ArcSight™

Reference Bits

Resources for Resources

- Packages UI
- Resource Graphs
- Archive tool
  - `$ARCSIGHT_HOME/bin/arcsight archive –h`
- Package tool
  - `$ARCSIGHT_HOME/bin/arcsight package -h`
- Handlers
  - `$ARCSIGHT_HOME/config/archive`
- DTDs
  - `$ARCSIGHT_HOME/schema/xml`

Specific Files of Interest

- `config/archive/default.xml`
  - Default import/export handler
- `config/archive/xml.external.case.xml`
  - Case/event export handler
- `schema/xml/archive/arcsight-archive.dtd`
  - Overall DTD for the resource archives
- `$ARCSIGHT_HOME/config/server.defaults.properties`
  - Default cache configurations
- `$ARCSIGHT_HOME/config/server.properties`
  - User configuration overrides

Include

- Include leniently, then prune with `<exclude>`
- `<include>`
  - explicitly include the resources and child resources of groups
- `<includeChildren>`
  - only bring along the children of the referenced group
- Framework supports other options, but these are the ones used in common practice

Exclude

- `<exclude>`
  - explicit, like include
- `<excludeChildren>`
  - useful for taking a group without any children
  - cases where you have multiple sub-archives
- `<excludeIfNotIncluded>`
  - useful when content is split into multiple archives/packages
  - often used for bringing along custom fields/DVs
- `<excludeChildrenIfNotIncluded>`
  - takes only children that are explicitly included
  - useful for resources that are linked into other content areas

Import Formats

- Choose based on the destination of the archive
- Typically chosen by the configuration in the archive/package
- Used by ArcSight internal folks who work on upgrades & patches
- Import formats allow us to specify options such as
  - Overwrite vs. merge
  - Preserve existing relationships vs. replace

And…

```
<SecurityEvent id="190000009134" name="Monitor Event" action="insert" >
  <agent>
   <map>
    <address>192.168.90.93</address>
    <assetId>4vD5c4RsBABCATpctsReNAQ==</assetId>
    <descriptorId>1</descriptorId>
    <hostName>192.168.90.93</hostName>
    <id>31T9c4RsBABCAV5ctsReNAQ==</id>
    <type>arcsight_security_manager</type>
    <version>4.5.0.0.0</version>
    <zone>
     <ref type="Zone" uri="/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 192.168.0.0-192.168.255.255”/>
    </zone>
   </map>
  </agent>
  <agentSeverity>Low</agentSeverity>
  <assetCriticality>0</assetCriticality>
```

Cache Sizes

- Classic problem, particularly when importing large numbers of Zones or Assets
- When importing, all resources are loaded into memory at once
- Can overflow the cache for a given resource type if you have a lot (e.g. thousands of Zones)
  - See `$ARCSIGHT_HOME/config/server.defaults.properties` (search on "`Resource Broker Configuration`")
  - As always, make changes to `server.properties`, NOT the "defaults" file
- Alternately, split your archives into multiple files and import separately
  - Best to try this first if reasonably possible

XML validation

- If you hand-edit archives, use an XML validator
  - The DTDs are included with the product for a reason
  - I use "`xmlvalid`" from ElCel because it works with on the command line in Cygwin & on *nix
  - http://www.elcel.com/products/xmltools/xmlvalid.html
- Many editors and programming environments also have XML validation modes

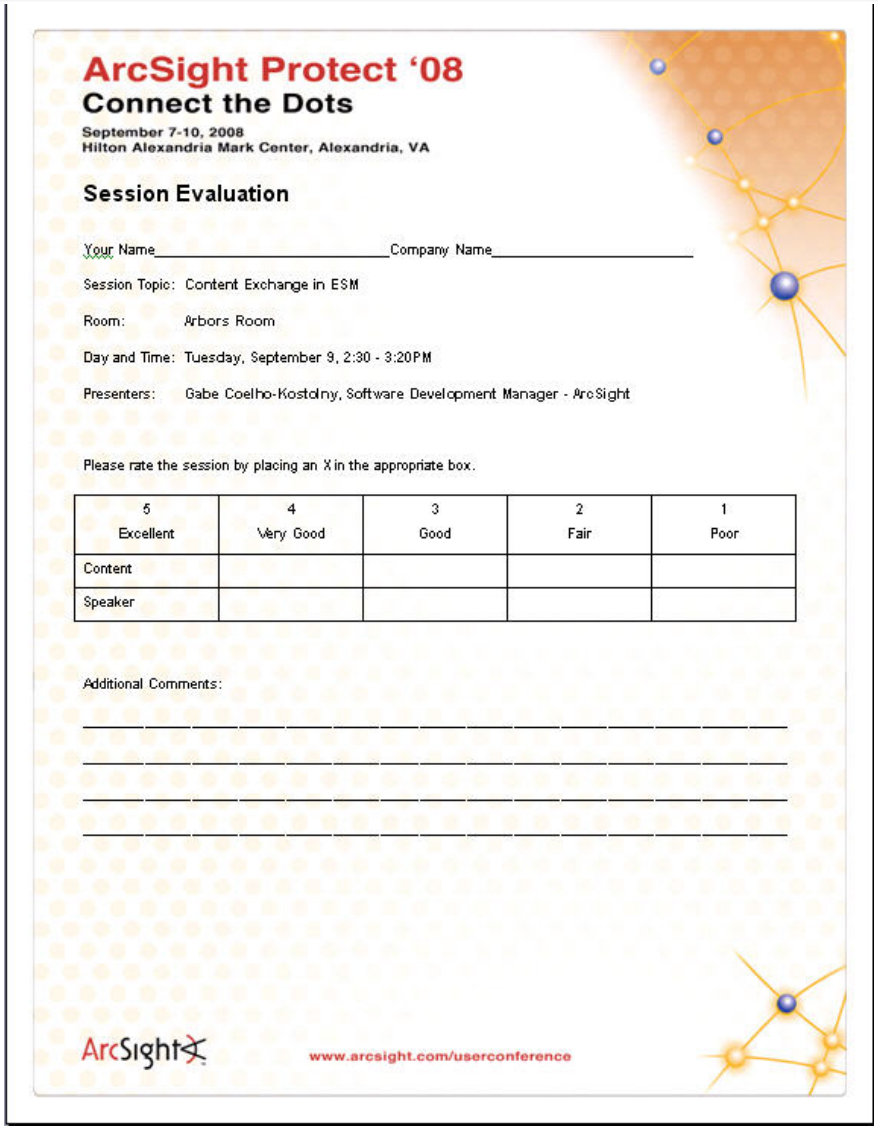
ArcSight™

For More Information

- ArcSight Inc.: www.arcsight.com
- Webcasts: www.arcsight.com/news_webinars.htm
- Collateral: www.arcsight.com/whitepapers.htm

Session Evaluation

- Please take a moment
  - to fill out our
  - session evaluation



ArcSight Protect '08
Connect the Dots
September 7-10, 2008
Hilton Alexandria Mark Center, Alexandria, VA

Session Evaluation

Your Name_____Company Name_____

Session Topic: Content Exchange in ESM

Room: Arbors Room

Day and Time: Tuesday, September 9, 2:30 - 3:20PM

Presenters: Gabe Coelho-Kostolny, Software Development Manager - ArcSight

Please rate the session by placing an X in the appropriate box.

	5 Excellent	4 Very Good	3 Good	2 Fair	1 Poor
Content					
Speaker					

Additional Comments:

_____

_____

_____

_____

ArcSight www.arcsight.com/userconference